UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

FINJAN, INC.,

Plaintiff,

v.

PROOFPOINT, INC., et al.,

Defendants.

Case No. 13-cv-05808-HSG

**CLAIM CONSTRUCTION ORDER**

Plaintiff Finjan, Inc. filed this patent infringement action against Defendants Proofpoint, Inc. and Armorize Technologies, Inc. The parties seek construction of seven claim terms found in six patents: Patent Nos. 6,154,844 ("the '844 Patent"), 7,058,822 ("the '822 Patent"), 7,647,633 ("the '633 Patent"), 7,975,305 ("the '305 Patent"), 8,141,154 ("the '154 Patent"), and 8,225,408 ("the '408 Patent"). This order follows claim construction briefing, a technology tutorial, and a claim construction hearing.

## I. LEGAL STANDARD

Claim construction is a question of law to be determined by the Court. *See Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995). "The purpose of claim construction is to determine the meaning and scope of the patent claims asserted to be infringed." *O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1360 (Fed. Cir. 2008) (internal quotation marks omitted).

Generally, claim terms should be given their ordinary and customary meaning—*i.e.*, the meaning that the terms would have to a person of ordinary skill in the art at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005) (en banc). There are only two circumstances where a claim is not entitled to its plain and ordinary meaning: "1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows

the full scope of a claim term either in the specification or during prosecution." *Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

When construing claim terms, the Federal Circuit emphasizes the importance of intrinsic evidence such as the language of the claims themselves, the specification, and the prosecution history. *Phillips*, 415 F.3d at 1312-17. The claim language can "provide substantial guidance as to the meaning of particular claim terms," both through the context in which the claim terms are used and by considering other claims in the same patent. *Id.* at 1314. The specification is likewise a crucial source of information. Although it is improper to read limitations from the specification into the claims, the specification is "the single best guide to the meaning of a disputed term." *Id.* at 1315 ("[T]he specification is always highly relevant to the claim construction analysis. Usually, it is dispositive.") (internal quotation marks omitted); *see also Merck & Co. v. Teva Pharms. USA, Inc.*, 347 F.3d 1367, 1371 (Fed. Cir. 2003) ("[C]laims must be construed so as to be consistent with the specification.").

Despite the importance of intrinsic evidence, courts may also consider extrinsic evidence—technical dictionaries, learned treatises, expert and inventor testimony, and the like—to help construe the claims. *Phillips*, 415 F.3d at 1317-18. For example, dictionaries may reveal what the ordinary and customary meaning of a term would have been to a person of ordinary skill in the art at the time of the invention. *Frans Nooren Afdichtingssystemen B.V. v. Stopaq Amcorr Inc.*, 744 F.3d 715, 722 (Fed. Cir. 2014) ("Terms generally carry their ordinary and customary meaning in the relevant field at the relevant time, as shown by reliable sources such as dictionaries, but they always must be understood in the context of the whole document—in particular, the specification (along with the prosecution history, if pertinent)."). Extrinsic evidence is, however, "less significant than the intrinsic record in determining the legally operative meaning of claim language." *Phillips*, 415 F.3d at 1317 (internal quotation marks omitted).

## II. AGREED TERMS

The parties have agreed to the construction of the following terms:

| Claim Term | Agreed Claim Construction |
|---|---|

| | |
|---|---|
| downloadable | an executable application program, which is downloaded from a source computer and run on the destination computer |
| security context | an environment in which a software application is run, which may limit resources that the application is permitted to access or operations that the application is permitted to perform |
| CODE-A | potentially malicious executable code |
| CODE-B | executable wrapper code |
| CODE-C | combined code |

*See* Dkt. No. 117. In light of the parties' agreement on the construction of these terms, the Court adopts the parties' constructions.

## III. DISPUTED TERMS

### A. '822 and '633 Patents

The '822 and '633 Patents share the same specification and are titled "Malicious Mobile Code Runtime Monitoring System and Methods." The inventions provide protection from "undesirable downloadable operation." '822 Patent at 1:25-29; '633 Patent at 1:30-33. Embodiments of the invention provide "for receiving downloadable-information and detecting whether the downloadable-information includes one or more instances of executable code." '822 Patent at 5:34-39. Where there is executable code, the invention provides

> **mobile protection code** ("MPC") and downloadable protection policies to be communicated to, installed and executed within one or more received **information destinations** in conjunction with a detected-Downloadable. Embodiments also provide, within an information-destination, for detecting malicious operations of the detected-Downloadable and causing responses thereto in accordance with the protection policies. . . .

*Id.* at 5:44-51 (emphases added). The parties dispute the meaning of the two bolded phrases.

#### 1. "mobile protection code"

| Finjan's Construction | Proofpoint's Construction |
|---|---|

| | |
|---|---|
| code capable of monitoring or intercepting potentially malicious code | code communicated to at least one information-destination that, at runtime, monitors or intercepts actually or potentially malicious code operations |

The parties agree that "mobile protection code" is not a term known in the art. Dkt. No. 142 at 5; Dkt. No. 170 at 57. Accordingly, the intrinsic record is the best evidence of the term's meaning. *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996) ("[A] patentee may choose to be his own lexicographer and use terms in a manner other than their ordinary meaning, as long as the special definition of the term is clearly stated in the patent specification or file history.").

In support of its construction, Plaintiff directs the Court to a portion of the specification indicating that "[t]he sandboxed package includes mobile protection code ("MPC") for causing one or more predetermined malicious operations or operation combinations of a Downloadable to be monitored or otherwise intercepted." '822 Patent at 3:6-10. Plaintiff argues that this passage provides an "explicit definition" of the term MPC, and demonstrates that MPC must merely be capable of monitoring or intercepting potentially malicious code. Dkt. No. 142 at 6.

Defendants' construction adds two limitations: (1) that MPC must monitor or intercept actually or potentially malicious code "at runtime" (*i.e.*, that is, monitoring potentially malicious code as the code is being executed), Dkt. No. 143 at 1-3, and (2) that MPC is "code communicated to at least one information-destination," *id.* at 4-5.

**a. "at runtime"**

The claims describe the execution of MPC as corresponding to "attempted operations" of the executable code at a downloadable-information destination. *See* '822 Patent at 22:63-67 (Claim 16); *id.* at 23:41-45 (Claim 27); '633 Patent at 22:1-5 (Claim 14); *id.* at 22:17-22 (Claim 20). Claim 28 of the '633 Patent describes the MPC receiving "operations attempted by the Downloadable" and "initiating, by the MPC on the computer, a protection policy corresponding to the attempted operation." '633 Patent at 22:55-63. And Claim 41 of the '633 Patent describes how the MPC initiates a "protection policy corresponding to the attempted operation." *Id.* at

24:30-34.[1] The Court finds that the claims' consistent description of correspondence with "attempted operations" by the downloadable indicates an "at runtime" limitation.

The specifications support this "at runtime" construction. First, the title of the patents is "Malicious Mobile Code **Runtime** Monitoring Systems and Methods." (emphasis added). The reference to "runtime" also is made in the first sentence of the "Detailed Description": "In providing malicious mobile code **runtime** monitoring systems and methods, embodiments of the invention enable actually or potentially undesirable operations of even unknown malicious code to be efficiently and flexibly avoided." '822 Patent at 5:30-31; '633 Patent at 5:30-31 (emphasis added).

Second, the specifications' description of when MPC is generated and initiated provides further support. The action generator generates MPC only when the protection engine determines that received downloadable information includes executable code, *see* '822 Patent at 9:24-26, 30-34; 12:18-65; Figs. 3 and 4. Upon such a determination, the protection engine "causes [MPC] to be communicated to the Downloadable-destination" by way of the transfer engine. *Id.* at 9:63-67; 14:38-43; 16:15-22. Figure 11 is instructive with regard to MPC's protection method within the destination device. MPC installs its elements and policies in the device and "forms an access monitor or 'interceptor' for monitoring or 'intercepting' downloadable destination device access attempts within the destination device." *Id.* at 20:21-30. When the monitored or intercepted information indicates that the downloadable is attempting to access the device in an undesirable way, MPC executes the protection policies. *Id.* at 20:33-40; *see also id.* at 20:54-56 (noting that MPC applies "suitable policies in accordance with an access attempt by a Downloadable"); *id*. at 18:42-47 (discussing MPC's resource access analyzer component "[d]uring downloadable operation").

The exemplary application of a sandbox package is further instructive:

> Upon receipt of sandboxed package by a compatible browser, email or other destination client and activating of the package by a user or

[1] *See also* '822 Patent at 24:5-11 (Claim 28) (describing the execution of MPC as "such that one or more operations of the executable code at the destination, if attempted, will be processed by the [MPC]."); *see also* '822 Patent at 24:39-43; '633 Patent at 22:28-34, 46-51; *Id.* at 23:21-28.

> the destination-client, **the operating system** (or a suitable responsively initiated distributed component host) **will attempt to initiate sandboxed package 340 as a single Downloadable. Such processing will, however, result in initiating the MPC 341** and-in accordance with further aspects of the invention-the MPC will initiate the Downloadable in a protected manner, further in accordance with any applicable included or further downloaded protection policies **342**.

*Id.* at 11:26-38 (emphasis added). Thus, the destination-client's receipt and activation of the sandboxed package causes MPC to initiate. Figure 7a also shows how the client's "attempt" to initiate the sandbox package in fact corresponds to "the beginning of the MPC"—the client recognizes the package as an executable and initiates the mobile code installer. *Id.* at 17:34-44. The mobile code installer then initiates MPC (not the downloadable), allowing MPC to form a protection "sandbox" around the downloadable, monitor the downloadable, and intercept malicious code. *Id.* at 17:45-59. These passages describing an illustrative embodiment of the invention confirm the Court's construction of the claim.

The Patents' references to MPC's monitoring functions in the present or past tense are also persuasive. *See id.* at 20:33-38 (MPC monitors whether "the Downloadable **is attempting** or **has attempted** a destination device access" (emphasis added)). The Abstract states the invention provides for "initiating the Downloadable [and] enabling malicious Downloadable operation **attempts** to be received by the MPC." *Id.* at Abstract (emphasis added). And the claims imply MPC only operates upon an "attempt" of the executable code. *See id.* at Claims 16, 28 (describing method whereby "operations of the executable code at the destination, **if attempted**, will be processed by the [MPC]" (emphasis added)); '633 Patent at Claim 14 (same). Defendants contend that there would be references to the future tense (*i.e.*, "will attempt") if MPC could monitor executable code before runtime and that the language shows that the executable code being monitored or intercepted must actually run (*i.e.*, make an attempt) to be received by the MPC. In light of the intrinsic evidence, the Court agrees.[2]

Plaintiff responds to Defendants' proposed construction by contending the specification

[2] Although not binding on this Court, *Finjan, Inc. v. Blue Coat Sys., Inc.*'s construction of MPC—that it operates "at runtime"—is further persuasive support for this Court's conclusion. *See* No. 13-CV-03999-BLF, 2014 WL 5361976, at *3 (N.D. Cal. Oct. 20, 2014).

demonstrates that protection policies exist as part of the static code in MPC, citing the Patent's "Summary of the Invention" in support:

> Embodiments also provide for delivering **static**, configurable and/or extensible remotely operable protection policies to a Downloadable-destination, more typically as a sandboxed package including the mobile protection code, downloadable policies and one or more received Downloadables.

'822 Patent at 2:42-47 (emphasis added). But, the Court is required to construe the claim term "in a way that comports with the instrument *as a whole*." *See Markman*, 517 U.S. at 389 (emphasis added). The invention's "Detailed Description" clarifies that "static" refers to the linking engine's formation of the sandboxed package, which includes initial and complete MPCs, other protection polices, and the downloadable. *Id.* at 13:31-36. The specification explains that the "[l]inking engine **405** is implementable in a static or configurable manner in accordance, for example, with characteristics of a particular user device/process stored intermittently or more persistently in storage **404**." *Id.* at 13:37-40. It goes on to explain that the linking engine is also configurable to form a protecting package that has more than one executable of the downloadable or to form

> an initial MPC, MPC-policy or sandboxed package (e.g. prior to upon receipt of a downloadable) or an additional MPC, MPC policy or sandboxed package (e.g. upon or following receipt of a downloadable), such that suitable MPCs/policies can be provided to a Downloadable-destination or other destination in a more distributed manner.

*Id.* at 14:1-7. That the linking engine allows for such varying static and configurable packaging options does not negate the intrinsic evidence confirming that MPC operates "at runtime."

**b. "code communicated to at least one information-destination"**

Defendants' second limitation requires that MPC be construed as "code communicated to at least one information-destination." Dkt. No. 142 at 4-5. Defendants argue the first word of the term MPC is "mobile," which means MPC must move somewhere. *Id.* ("The Court should further conclude . . . that mobile protection code is **mobile**" (emphasis in original)). But the phrase "communicated to at least one information-destination" does not appear anywhere in the specification. Instead, it appears in some—but not all—of the patents' claims. *Compare* '633 Patent at 21:48-55 (disclosing "[a] processor-based system . . . causing [MPC] to be

communicated to at least one information-destination . . . .") *with id.* at 21:58-22:5 ("[a] computer program product . . . causing [MPC] to be executed by the mobile code executor at a downloadable-information destination . . ."). If MPC, by definition, needed to be communicated to at least one information-destination, the inclusion of that language in any of the claims would be redundant.

Moreover, the Court is not persuaded by Defendants' argument that Plaintiff expressly disclaimed its preferred construction during the prosecution of the '633 Patent. Dkt. No. 142 at 5 (quoting language from '633 Patent's prosecution history in which Plaintiff stated that "[t]he claimed invention provides a packaging of mobile protection code with a downloadable intended for a destination computer . . . . In distinction with the claimed invention, Golan does not describe the packaging of protection code. Instead, Golan discusses a situation whereby a security monitor is already resident on a client computer . . . ."). It is not clear and unambiguous that Plaintiff's distinction between Golan's invention and the'633 Patent's invention was based on the "communication" of MPC to an information-destination. *See Verizon Servs. Corp. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1306 (Fed. Cir. 2007) ("To operate as a disclaimer, the statement in the prosecution history must be clear and unambiguous, and constitute a clear disavowal of scope."). Because the disavowal is not unambiguous, the Court declines to adopt Defendants' second limitation.

Accordingly, the Court construes "mobile protection code" as "code that, at runtime, monitors or intercepts actually or potentially malicious code operations."

**2. "information-destination/downloadable-information destination"**

| Finjan's Construction | Proofpoint's Construction |
|---|---|
| no construction necessary—Plain and ordinary meaning | a user device that receives and initiates (or otherwise hosts) execution of the downloadable information |

Plaintiff contends that these terms are explicitly defined in the '822 Patent as "any server or computer where the information is communicated to, installed or executed." Dkt. No. 142 at 23 (citing '822 Patent at 5:44-48). Contrary to Plaintiff's description of the specification, the passage

it cites does not provide that an information destination is "any server or computer where the information is communicated to, installed, ***or*** executed." Instead, the passage uses the conjunctive "and":

> Embodiments further provide for causing mobile protection code ("MPC") and downloadable protection policies to be communicated to, installed ***and*** executed within one or more received information destinations in conjunction with a detected-Downloadable.

'822 Patent at 5:44-48 (emphasis added). At the claim construction hearing when questioned about the difference between the specification and the quoted passage, Plaintiff insisted that under its construction an information-destination "does not have to be a location where it has be executed." Dkt. No. 170 at 49.

Defendants argue that the specification defines the terms more narrowly, requiring a "user device . . . that [is] capable of receiving and initiating or otherwise hosting a mobile code execution." Dkt. No. 143 at 7 (quoting '822 Patent 7:60-65).

The Court finds that the passages the parties cited mostly support Defendants' construction. The specification's language is dispositive:

> A suitable information-destination or 'user device' can further include one or more devices or processes (such as email, browser or other clients) that are capable of receiving and initiating or otherwise hosting a mobile code execution.

'822 Patent at 7:60-65. *Vitronics*, 90 F.3d at 1582 ("The specification acts as a dictionary when it expressly defines terms used in the claims or when it defines terms by implication.").

Thus, consistent with the intrinsic evidence, the Court construes "information-destination" and "downloadable-information destination" as "a device or process that is capable of receiving and initiating or otherwise hosting a mobile code execution."

**B. '408 Patent**

The '408 Patent, titled "Method and System For Adaptive Rule-Based Content Scanners," covers "a method and system for scanning content that includes mobile code, to produce a diagnostic analysis of potential exploits within the content." '408 Patent at 1:59-61. The invention uses an adaptive rule-based content ("ARB") scanner, which dynamically scans and diagnoses incoming Internet content. *Id.* at 1:65-2:24. The system generates a parse tree based on tokens and patterns of

tokens it identifies, then identifies exploits (the malicious portions of the code) within the parse tree. *Id.* at 2:25-57.

**3. "parse tree"**

| Finjan's Construction[3] | Proofpoint's Construction |
|---|---|
| a way of organizing exploits in scanned content into a hierarchical structure with one root and several branches, much like a family tree or genealogy chart. | a set of nodes linked in a hierarchy that represents a sequence of words and symbols according to a given syntax. |

The claim term appears in claims 1, 2, 9, 11, and 22-35 of the '408 Patent. Independent claim 1 describes:

> A computer processor-based multi-lingual method for scanning incoming program code, comprising:
>
> receiving, by a computer, an incoming stream of program code; determining, by the computer, any specific one of a plurality of programming languages in which the incoming stream is written;
>
> instantiating, by the computer, a scanner for the specific programming language, in response to said determining, the scanner comprising parser rules and analyzer rules for the specific programming language, wherein the parser rules define certain patterns in terms of tokens, tokens being lexical constructs for the specific programming language, and wherein the analyzer rules identify certain combinations of tokens and patterns as being indicators of potential exploits, exploits being portions of program code that are malicious;
>
> identifying, by the computer, individual tokens within the incoming stream;
>
> dynamically building, by the computer while said receiving receives the incoming stream, a **parse tree** whose nodes represent tokens and patterns in accordance with the parser rules;
>
> dynamically detecting, by the computer while said dynamically building builds the **parse tree**, combinations of nodes in the parse tree which are indicators of potential exploits, based on the analyzer rules;
>
> and indicating, by the computer, the presence of potential exploits within the incoming stream, based on said dynamically detecting.

[3] Plaintiff's initial construction was "a tree data structure representing exploits in scanned content." Defendants' initial construction was "a set of linked nodes whose nodes represent tokens and patterns in accordance with the parser rules." Each party revised its proposed construction in supplemental briefing filed after the claim construction hearing.

'408 Patent, 19:45-20:7 (emphases added).

Plaintiff's construction incorporates the limitation that a parse tree applies to "exploits in scanned content" whereas Defendants' construction describes "a sequence of words and symbols according to a given syntax" without any mention of "scanned content" generally or exploits from the scanned content, specifically. The Court rejects both proposals.

There are two problems with Plaintiff's construction. First, although the parse tree can be used to identify exploits, it is not limited to this use. Parsing rules can be used to perform various actions, such as "setting internal variables; invoking a sub-scanner **270**, . . . and searching the parse tree for nodes satisfying specific conditions." *Id.* at 8:61-66. Second, while one action of the parse tree is to identify exploits, that action is not a requisite characteristic of a parse tree. The term's construction does not need to include all of the parse tree's uses; it only need describe what the parse tree is. At its core, the parse tree provides a means of organizing and presenting data—for example, each node preferably contains "data indicating inter alia an ID number, the token or rule that the node represents, a character string name as a value for the node, and a numerical list of attributes." *Id.* at 8:38-41.

Defendants' construction is similarly flawed. The construction imports the limitation that nodes represent "a sequence of words and symbols according to a given syntax." But, the definition of parse tree does not need to include an explanation of what the nodes represent. There is no evidence—intrinsic or extrinsic—that a parse tree stops being a parse tree if the nodes were to represent something other than a sequence of words and symbols.

On the other hand, the claims impose three requirements that the Court concludes must be a part of the term's construction. First, a parse tree is "built." Claim 1 describes the actions of "**dynamically building**, by the computer while said receiving receives the incoming stream, a parse tree" and "dynamically detecting, by computer while **said dynamically building builds the parse tree**," *id.* at 19:64-66; 20:1-3 (emphasis added); *see id.* at 20:8-9 (Claim 2) (describing a method "wherein said dynamically building a parse tree is based upon a shift-and-reduce algorithm"). Independent Claim 9 also describes the parser "dynamically building the parse tree." *Id.* at 21:1-2. The specifications further confirm this construction—"the parse tree generated by

parser **220** is dynamically built using a shift-and-reduce algorithm," *id.* at 8:29-30, and "[i]t may thus be appreciated that the analyzer is called repeatedly, while the parse tree is being dynamically built up," *id.* at 14:53-55; *see id.* at 9:64-66.

Second, a parse tree is built from "scanned content." Claim 1 describes the parse tree as "identifying . . . individual tokens **within the incoming stream**; dynamically building, by the computer while said receiving **receives the incoming stream**, a parse tree whose nodes represent tokens," *id.* at 19:62-66 (emphases added). Claim 9 describes "a parser, for dynamically building while said receiver is receiving **the incoming stream**, a parse tree," *id.* at 9:64-66 (emphasis added). The specifications also confirm this construction—"[T]he present invention is able to diagnose incoming content." *Id.* at 2:20-21. The "parser controls the process of scanning incoming content," *id.* at 8:19-20, and the "parser **220** uses a parse tree data structure to represent scanned content," *id.* at 8:24-25.

Third, a parse tree is a "hierarchical structure of interconnected nodes." Claims 24 and 30 illustrate the "interconnected" nature of the nodes—that the "parser positions nodes of the parse tree corresponding to rules as parent nodes, the children of which correspond to tokens within the patterns that correspond to the rules." *Id.* at 22:28-32; 23:22-25. Figure 2 from the written description is instructive. The block diagram is an embodiment of the ARB scanner and shows the parse tree as a hierarchical structure with connected nodes.

Here, both parties agree that a parse tree must be hierarchical, *see* Dkt. No. 166 at 2-3 (citing extrinsic evidence); Dkt. No. 168 at 2-3 (same). Their understanding is consistent with the Patent's specification. The specification describes an embodiment that builds the parse tree using a "shift-and-reduce algorithm," *id.* at 8:29-30, invoking the image of a hierarchical structure with nodes that are shifted over and moved down depending on their relationships to each other. The parser automatically performs "a reduce operation by creating a new node and moving token nodes underneath the new node" whenever a pattern is matched within the parser rule. *Id.* at 8:66-9:2.

Moreover, the specification describes the tokens' relationships to each other and the fact that they are built on each other. For instance, the parser's method describes connecting the

tokens based on parent-child and sibling relationships—

> Successive tokens provided to parser **220** by tokenizer **210** are positioned as siblings. When parser **220** discovers that a parsing rule identifies a group of siblings as a single pattern, the siblings are reduced to a single parent node by positioning a new parent node, which represents the pattern, in their place, and moving them down one generation under the new parent note.

*Id.* at 8:30-37.

Accordingly, the Court construes claim term "parse tree," in light of the intrinsic evidence, as "a hierarchical structure of interconnected nodes built from scanned content."

### C. The '154 Patent

The '154 Patent, titled "System and Method for Inspecting Dynamically Generated Executable Code," concerns "new behavioral analysis technology that affords protection against dynamically generated malicious code," which are those viruses generated at runtime. '154 Patent at 4:32-34; 3:32-33. Behavioral analysis technology is able to block these "viruses that have not been previously detected and which do not have a signature on record." *Id.* at 1:62-64.

#### 1. "a call to a first function . . . [invoking/invoke/calling] a second function"

| Finjan's Construction | Proofpoint's Construction |
|---|---|
| no construction necessary—plain and ordinary meaning | a call to a function different from the second function . . . [invoking/ invoke/ calling] a function different from the first function |

The disputed language appears in Claims 1, 4, 6, and 10 of the '154 Patent. Independent Claim 1 of the '154 Patent is representative of how the term is used in the claim language:

> a content processor (i) for processing content received over a network, the content including **a call to a first function**, and the call including an input, and (ii) for **invoking a second function** with the input, only if a security computer indicates that such invocation is safe;

'154 Patent at 17:34-38 (emphases added). The parties' sole dispute concerning this term is whether the "first function" and the "second function" can be the same function. Plaintiff argues that "first" and "second" identify the order in which the functions are called, while Defendants argue that "first" and "second" indicate that they must be different functions.

Defendants' argument has no support in the '154 Patent's claims. Nothing in the claim

language precludes the first and second function from being the same function. Defendants rely on the specification language, however, which describes the "first" and "second" functions as "original" and "substitute."

> To enable the client computer to pass function inputs to the security computer and suspend processing of content pending replies from the security computer, the present invention operates by **replacing original function calls with substitute function calls** within the content, at a gateway computer, prior to the content being received at the client computer.

'154 Patent at 4:55-60 (emphasis added).

Defendants contend that the specifications would not have described the functions as "original" and "substitute" functions if those functions were identical. Plaintiff responds that Defendants are mistaken when they equate the second function identified in the claims and the substitute function identified in the specification. Specifically, Plaintiff notes that the second function is invoked only *after* the security computer indicates that the invocation is safe, while the original function is replaced by the substitute function at the gateway, *before* the security computer receives the content. *See also id*. at Fig. 2. As the specification explains, the invention discloses:

> content being sent to a client computer for processing, the content including a call to an original function, and the call including an input, **modifying the content <u>at the gateway computer</u>, including replacing the call to the original function with a corresponding call to a substitute function**, the substitute function being operational to send the input to a security computer for inspection, transmitting the modified content from the gateway computer to the client computer, processing the modified content at the client computer, transmitting the input to the security computer for inspection when the substitute function is invoked . . .

*Id*. at 5:4-18 (emphasis added). The specification is clear that it is the original function—not the substitute function—that is invoked after the security computer determines that its invocation is safe. The specification continues:

> determining at the security computer whether it is safe for the client computer to invoke the original function with the input, transmitting an indicator of whether it is safe for the client computer to invoke the original function with the input, from the security computer to the client computer, and **invoking the <u>original function</u> at the client computer with the input, only if the indicator received from the security computer indicates that such invocation is**

**safe**.

*Id*. at 5:18-25 (emphasis added). The Court agrees that this passage of the specification demonstrates that the "second function" described in the claims can be the "original function" identified in the specification.[4] *See Chef Am., Inc. v. Lamb-Weston, Inc*., 358 F.3d 1371, 1373 (Fed. Cir. 2004) ("These are ordinary, simple English words whose meaning is clear and unquestionable. . . .They mean exactly what they say.").

Accordingly, the Court concludes that the specification does not support Defendants' argument that the first and second functions must be different. The term's plain and ordinary meaning governs, and no construction is necessary. *See Phillips*, 415 F.3d at 1312 ("[T]he words of a claim are generally given their ordinary and customary meaning.").

**2. "content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if security computer indicates that such invocation is safe"**

| Finjan's Construction | Proofpoint's Construction |
|---|---|
| no construction necessary—plain and ordinary meaning | means-plus-function under § 112, ¶ 6<br><br>**Function**: processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if security computer indicates that such invocation is safe<br><br>**Structure**: the algorithm performed by a web browser running on client computer 210, 410 and described in col. 10, l. 30 - col. 11, l. 4; as well as shown in Fig. 3 (steps 324-335, 384-392) and described in col. 13, l. 63 - col. 14, l. 16 and col. 14, l. 61 - col. 15, l. 3; as well as shown in Fig. 5 (steps 525-540, 585-595) and described in col. 16, ll. 22-32, 62-67. |

The disputed language appears in independent Claim 1 of the '154 Patent. It reads:

a content processor (i) for processing content received over a

[4] Moreover, the Federal Circuit has repeatedly warned courts that "it is the claims, not the written description, which define the scope of the patent right." *Laitram Corp. v. NEC Corp.*, 163 F.3d 1342, 1347 (Fed. Cir. 1998) ("[A] court may not import limitations from the written description into the claims."). Here, the claims do not use "original" and "substitute" functions.

> network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe;

'154 Patent at 17:34-38. The parties dispute whether the phrase "content processor for processing . . . and for invoking" is a means-plus-function claim that must be construed under 35 U.S.C. § 112, ¶ 6. Defendants contend that it is. Dkt. No. 143 at 20. Section 112, ¶ 6 provides:

> An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

§ 112. Plaintiff argues that the limitation is not a means-plus-function claim and that no construction is necessary, as a person of ordinary skill in the art would understand the term as it appears in the claim and in light of the specification. Dkt. No. 142 at 20.

To determine whether a claim invokes § 112, the Court must determine if the claim limitation is drafted in the means-plus-function format. "The use of the term 'means' triggers a rebuttable presumption that § 112, ¶ 6 governs the construction of the claim term." *Robert Bosch, LLC v. Snap-On Inc.*, 769 F.3d 1094, 1097 (Fed. Cir. 2014) (citations omitted). There is a general presumption that the limitation does not invoke § 112, ¶ 6 where the claim language does not recite the term "means." *Id.* The presumption is rebuttable.

Before this year, the presumption that § 112 does not apply when a claim term does not use "means" was "a strong one that [was] not readily overcome," *see Lighting World, Inc. v. Birchwood Lighting, Inc.*, 382 F.3d 1354, 1358 (Fed. Cir. 2004), *overruled by Williamson v. Citrix Online, LLC*, 792 F.3d 1339 (Fed. Cir. 2015). The Federal Circuit recently clarified, however, that "such a heightened burden is unjustified" and "expressly overrule[d] the characterization of that presumption as strong." *Williamson*, 792 F.3d at 1349. Instead, courts must ask whether "the words of the claim are understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure." *Id.* If a "term lacks the word 'means,' the presumption can be overcome and § 112, para. 6 will apply if the challenger demonstrates that the claim term fails to 'recite sufficiently definite structure' or else recites 'function without reciting sufficient structure for performing that function.'" *Id.*

Both parties agree that the word "means" does not appear in the claim language. Dkt. No. 142 at 20; Dkt. No. 143 at 20. Accordingly, the Court finds that the presumption against invoking § 112, ¶ 6 applies to this language. Defendants have not demonstrated that the claim term "fails to recite sufficiently definite structure" or else "recites function without reciting sufficient structure for performing that function" so as to overcome this presumption. *See Robert Bosch, LLC*, 769 F.3d at 1097; *Williamson*, 792 F.3d at 1349.

The term "content processor" has a sufficiently specific structure. Independent Claim 1 describes how the "content processor" interacts with the invention's other components (the transmitter and receiver), which informs the term's structural character. '154 Patent at 17:32-44, 18:7-22; *see also id.* at 17:45-49 ("[S]aid content processor (i) suspends processing of the content after said transmitter transmits the input to the security computer, and (ii) resumes processing of the content after said receiver receives the indicator from the security computer.").

The specification identifies where the component is located—"Gateway computer **205** includes a content modifier **265**, client computer **210** includes a content processor **270**, and security computer **215** includes an inspector." *Id.* at 9:8-10; *see also id.* at 15:33-36 ("Client computer **410** includes a content processor **470**, such as a web browser, which processes content received from the network.").

Figures 2 and 3 of the '154 Patent are also instructive. The block diagrams illustrate the content processor's location and its relationship to other components. *See Inventio AG v. ThyssenKrupp Elevator Americas Corp.*, 649 F.3d 1350, 1358 (Fed. Cir. 2011) (holding that the term was not purely functional where "the written descriptions depict the modernizing device and its internal components, namely, the processor, signal generator, converter, memory, and signal receiver elements" and show how the elements are connected together), *overruled by Williamson*, 792 F.3d at 1349. Unlike *Williamson*, where the term "module" was "simply a generic description for software or hardware that performs a specified function," *see id.* at 1350, here, the intrinsic evidence establishes the structural character of "content processor" through its interaction with the system's other components.

Because the intrinsic evidence describes the term's location and its interactions with other

components, the means-plus-function limitation does not apply. Thus, the term does not require any construction beyond its plain and ordinary meaning.

### D. The '305 Patent

The '305 Patent, titled "Method and System for Adaptive Rule-Based Content Scanners for Desktop Computers," covers a method and system for receiving and scanning Internet content to produce a diagnostic analysis of potential exploits within the mobile code. '305 Patent 1:64-2:9. The invention analyzes incoming content in terms of its programmatic behavior; this behavioral analysis "is an automated process that parses and diagnoses a software program, to determine if such program can carry out an exploit." *Id.* at 1:66-2:3.

#### 1. "selectively diverting incoming content from its intended destination to said rule-based content scanner"

| Finjan's Construction | Proofpoint's Construction |
|---|---|
| no construction necessary—Plain and ordinary meaning | indefinite |

Independent claim 1 describes:

> A security system for scanning content within a computer, comprising:
>
> a network interface, housed within a computer, for receiving incoming content from the Internet on its destination to an Internet application running on the computer;
>
> a database of parser and analyzer rules corresponding to computer exploits, stored within the computer, computer exploits being portions of program code that are malicious, wherein the parser and analyzer rules describe computer exploits as patterns of types of tokens, tokens being program code constructs, and types of tokens comprising a punctuation type, an identifier type and a function type;
>
> a rule-based content scanner that communicates with said database of parser and analyzer rules, operatively coupled with said network interface, for scanning incoming content received by said network interface to recognize the presence of potential computer exploits therewithin;
>
> a network traffic probe, operatively coupled to said network interface and to said rule-based content scanner, **for selectively diverting incoming content from its intended destination to said rule-based content scanner** . . . .

'305 Patent 29:44-66 (emphasis added).

Although the parties agree that "selectively diverting" requires that some content "is selected to be diverted from" its intended destination to the scanner, Dkt. No. 142 at 22; Dkt. No. 143 at 23, they dispute whether the term is indefinite in light of the specification. Defendants contend that the sheer scope of the ordinary meaning of "selectively"—"when items are selected"—renders the claim indefinite. For example, Defendants observe that "[t]he term 'selectively' suggests that there exists some criteria for choosing what is diverted, but provides no guidance on what constitutes acceptable criteria." Dkt. No. 143 at 11.

"[A] patent is invalid for indefiniteness if its claims, read in light of the specification delineating the patent, and the prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014). "The definiteness requirement, so understood, mandates clarity, while recognizing that absolute precision is unattainable." *Id.* at 2129.

The Court concludes that the term, read in light of the intrinsic evidence, is reasonably definite insofar as it informs those skilled in the art about the scope of the invention with reasonable certainty. As described in Claim 1 and illustrated in Figure 9, a "network traffic probe" is "operatively coupled" to both the network interface, which receives the incoming content, and the rule-based scanner, which uses parser and analyzer rules to scan incoming content. '305 Patent at 2:37-52. The specification describes the process for "selectively diverting." First, the "network gateway **110** [ ] acts as a conduit for content from the Internet entering into a corporate intranet." *Id.* at 5:43-47; Fig. 1. "Preferably, network gateway **110** checks if incoming content is already resident in cache **140**, and, if so, bypasses content scanner **130**." *Id.* at 7:36-40. Thus, if the scanned content and their corresponding security profiles are in the content cache, then that content is not selectively diverted to the ARB scanner. *Id.* Second, the pre-scanner—which "uses conventional signature technology to scan content," *id.* at 8:5-6—identifies whether the network traffic probe should divert specific content to the ARB scanner:

> pre-scanner **150** acts as a first-pass filter, to filter content that can be quickly recognized as innocuous. Content that is screened by pre-scanner **150** as being potentially malicious is passed along to ARB scanner **130** for further diagnosis. Content that is screened by pre-scanner **150** as being innocuous bypasses ARB scanner **130**. It is

> expected that pre-scanner **150** filters 90% of incoming content, and that only 10% of the content requires extensive scanning by ARB scanner **130**.

*Id.* at 8:17-25. The passage clarifies that the network traffic probe diverts only the content that the pre-scanner determines is potentially malicious, which corresponds to about 10 percent of incoming content. Given this intrinsic evidence, Defendants' contention—that it is unclear whether diverting files at random or diverting every third file would constitute "selectively diverting"—is unsupported. *See Nautilus*, 134 S. Ct. at 2123 (recognizing that "absolute precision is unattainable"); *Enzo Biochem, Inc. v. Applera Corp.*, 599 F.3d 1325, 1335 (Fed. Cir. 2010) (holding that claim "not interfering substantially" was not indefinite even though the construction "define[d] the term without reference to a precise numerical measurement"). Although the specification describes the invention with reference to exemplary embodiments, the cited passages sufficiently define the claim's scope: they establish that "selectively diverting" is not a subjective process, but rather a defined one in which content is diverted based on the presence of potential exploits.

Additionally, the Court agrees with Plaintiff that the claim's use of the term "selectively diverting" aligns with the term's ordinary meaning understandable to those skilled in the art. *See* Dkt. No. 142 at 22 (relying on expert's testimony that "a person of ordinary skill in the art would understand the meaning of the term 'selectively diverting incoming content from its intended destination to said rule-based content scanner' with reasonable certainty . . . ." (citing Dkt. No. 142-1 at ¶ 47-56)); *Fortinet, Inc. v. Sophos, Inc.*, No. C-13-5831 EMC, 2015 WL 877410, at *1 (N.D. Cal. Feb. 27, 2015) (holding where the ordinary meaning of claim language "is readily apparent . . . claim construction in such cases involves little more than the application of the widely accepted meaning of commonly understood words" (internal quotation marks and citation omitted)).

The Court finds that the claims, viewed in light of the specifications, "inform those skilled in the art about the scope of the invention with reasonable certainty," and that the term "selectively diverting" is definite. *See Nautilus*, 134 S.Ct. at 2129. The Court also finds that the plain and ordinary meaning of "selectively diverting" is consistent with the specification and that no

construction is necessary.

**E. The '844 Patent**

The '844 Patent, titled "System and Method for Attaching a Downloadable Security Profile to a Downloadable," facilitates the protection of computers and networks from a hostile Downloadable." '844 Patent at 1:23-27. A downloadable application, or downloadable, is "an executable application program, which is downloaded from a source computer and run on the destination computer." *Id.* at 1:44-47. "The network system includes an inspector for linking Downloadable security profiles to a Downloadable, and a protection engine for examining the Downloadable and Downloadable security profiles to determine whether or not to trust the Downloadable security profiles." *Id.* at 1:65-2:2. The invention provides for:

> a method in a first embodiment comprising the steps of receiving a Downloadable, generating a first Downloadable security profile for the received Downloadable, and linking the first Downloadable security profile to the Downloadable . . . [and] a method in a second embodiment comprising the steps of receiving a Downloadable with a linked first Downloadable security profile, determining whether to trust the first Downloadable security profile, and comparing the first Downloadable security profile against the security policy if the first Downloadable.

*Id.* at 2:49-60.

**1. "linking the first Downloadable security profile to the Downloadable"**

| Finjan's Construction | Proofpoint's Construction |
|---|---|
| No construction necessary—Plain and ordinary meaning | creating an association from the Downloadable to the first Downloadable security profile, including using a pointer from the Downloadable to the profile or attaching the profile to the Downloadable |

**"downloadable [includes / with] a linked [first] Downloadable security profile"**

| Finjan's Construction | Proofpoint's Construction |
|---|---|
| No construction necessary—plain and ordinary meaning | Downloadable [includes / with] an association to a [first] Downloadable security profile, including using a pointer from the Downloadable to the profile or attaching the profile to the |

| | |
|---|---|
| | Downloadable |

The parties agree that the '844 Patent describes "linking" as creating an association between the Downloadable and its Downloadable security profile ("DSP").

> The term "linking" herein will be used to indicate an association between the Downloadable **205** and the DSP **215** (including using a pointer from the Downloadable **195** to the DSP **215**, attaching the DSP **215** to the Downloadable **205**, etc.)

'844 Patent at 6:20-24. The parties disagree as to whether the construction of the term "linking" or "linked" should be limited to the two examples in the specification.

The Court agrees that the '844 patent expressly defines the term "linking," and that "the patentee's lexicography must govern the claim construction analysis." *Braintree Labs., Inc. v. Novel Labs, Inc.*, 749 F.3d 1349, 1356 (Fed. Cir. 2014). The Court finds that the definition of "linking" is not limited to the examples identified or even to all potential associations included in the Downloadable itself. The remainder of the cited passage is instructive:

> Although the signed inspected Downloadable **195** illustrates the DSP **215** (and Downloadable ID **220**) as an attachment, one skilled in the art will recognize that the DSP **215** can be linked to the Downloadable **205** using other techniques. For example, the DSP **215** can be stored in the network system **100**, and alternatively a pointer to the DSP **215** can be attached to the signed inspected Downloadable **195**.

'844 Patent at 6:13-20. The '844 Patent does not limit the word "association" in any way. *Hill-Rom Servs., Inc. v. Stryker Corp.*, 755 F.3d 1367, 1372 (Fed. Cir.) *cert. denied*, 135 S. Ct. 719 (2014) ("Even when the specification describes only a single embodiment, the claims of the patent will not be read restrictively unless the patentee has demonstrated a clear intention to limit the claim scope using 'words or expressions of manifest exclusion or restriction.'" (citation omitted)). The two examples in the specification are only examples. That both examples involve creating an association within the Downloadable itself (either by using a pointer or attaching the DSP to the Downloadable) does not exclude all other methods of associating a Downloadable to a DSP. This is especially true considering the use of "etc." at the end of the definition. '844 Patent at 6:24.

Finally, the '844 Patent's express definition of "linking" as "association" does not add anything to the plain and ordinary meaning of "linking." Thus, the Court concludes that the plain and ordinary meaning of "linking" governs, that the term is not limited to the exemplar methods in

the definition, and that no construction is necessary.

## IV. CONCLUSION

The Court construes the disputed terms as follows:

| Term | Patent(s) | Construction |
|---|---|---|
| mobile protection code | '633 and '822 Patents | code that, at runtime, monitors or intercepts actually or potentially malicious code operations |
| information-destination/downloadable-information destination | '633 and '822 Patents | a device or process that is capable of receiving and initiating or otherwise hosting a mobile code execution |
| parse tree | '408 Patent | a hierarchical structure of interconnected nodes built from scanned content |
| a call to a first function . . . [invoking/invoke/calling] a second function | '154 Patent | plain and ordinary meaning; no construction necessary |
| content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if security computer indicates that such invocation is safe | '154 Patent | plain and ordinary meaning; no construction necessary |
| selectively diverting incoming content from its intended destination to said rule-based content scanner | '305 Patent | plain and ordinary meaning; no construction necessary |
| linking/linked, as used in: Linking the first Downloadable security profile to the Downloadable Downloadable [includes / with] a linked [first] Downloadable security profile | '844 Patent | plain and ordinary meaning; no construction necessary |

**IT IS SO ORDERED.**

Dated: 12/3/2015

HAYWOOD S. GILLIAM, JR.
United States District Judge